Асимптотически оптимальный метод встраивания скрытой информации в стегосистемах

АВТОРЫ: д.т.н. Рябко Б. Я., д.т.н. Фионов А. Н.

Объект исследования – стеганографические системы. Предмет исследования – поиск асимптотически оптимальных методов внедрения скрытой информации.

Во многих практически используемых стегосистемах встраивание скрытых данных в цифровой объект (изображение, видео, аудио и т.п.), называемый контейнером, производится путем внесения небольших искажений в первоначальные данные. Обозначим через D множество допустимых искажений (мы считаем допустимыми искажения, которые не могут быть обнаружены с помощью известных методов стегоанализа). Тогда емкость стегосистемы (максимальное количество внедряемой информации) $\gamma \le \log|D|$. Пусть $\lambda(\cdot)$ – линейная хеш-функция, обладающая свойством $\lambda(c \oplus d) = \lambda(c) \oplus \lambda(d)$, где c и d – двоичные последовательности одинаковой длины.

Предлагается следующая схема встраивания сообщения s в контейнер c: вычисляем $u = \lambda(c)$, $v = u \oplus s$, находим искажение $d \in D$ такое, что $\lambda(d) = v$, получаем стеготекст (контейнер с внедренным сообщением) $w = c \oplus d$. Извлечение скрытых данных производится путем вычисления хеш-функции от стеготекста: $s = \lambda(w)$.

Предложена конструкция линейной хеш-функции, основанная на свойствах бинарных полей (полей Галуа). Показано, что для некоторых практически важных конфигураций множеств допустимых искажений полученная стегосистема достигает предельной емкости внедрения.

Получен результат, касающийся потенциальной емкости стегосистемы, построенной на базе линейной хеш-функции, который формулируется как следующая

Теорема. Для больших $|D|$ и любого $\delta > 0$ неравенство

$$\gamma_\lambda \ge \log|D| - \log\ \ln\ (|D|/\delta)$$

справедливо с вероятностью $1-\delta$, т.е. стегосистема является асимптотически оптимальной.

Похожие по своим свойствам стегосистемы, способные реализовывать лишь некоторые множества искажений, строились на базе кодов, исправляющих ошибки. В данном исследовании впервые построен асимптотически оптимальный метод встраивания данных, который позволяет значительно расширить класс множеств допустимых искажений и увеличить количество скрытно внедряемой информации. Данный результат важен для решения классических задач стеганографии, а также для задач защиты авторского права, защиты от несанкционированного копирования и др.

ПУБЛИКАЦИИ:

1. Рябко Б.Я., Фионов А.Н. Метод сокрытия информации, основанный на использовании линейной функции хэширования // IX Симпозиум "Современные тенденции в криптографии", Калининград, 4–7 июня, 2019.
2. Ryabko B., Fionov A. Linear hash functions as a means of distortion--rate optimization in data embedding // Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'19), Paris, France, July 03 - 05, 2019. P. 235–238. (Scopus).